cyber eco

Incident Management Guide

For SMB

October 28th, 2021

Sebastien Harbec

A word about the author

Working in the field of cyber security for various industries since 2007, I have come to the realization that cybersecurity is only as efficient as the bond uniting the people, processes and technologies behind it. Prevention, detection and reaction to cyberattacks succeed only when they take into account businesses' and people's realities.

To hone my strategic approach, I decided to pursuit a graduate degree in cyber security at Université de Sherbrooke. While studying reactive cyber security, my graduation project prompted me to ponder security issues for smaller structures. The idea of helping SMB automatically came to mind.

IT security for SMB, not just in Québec but also around the world, is a matter of great concern. Small and medium-sized companies form the social and economic fabric of a healthy market. Given the proliferation of cyber attacks, it is becoming more important than ever to give SMB the tools to handle them. Few emerge unscathed from such ordeals.

This guide provides practical advice in the event of a cyber attack and solutions to deal with incidents. It is not a substitute for the advice and support of an expert, but it does offer immediate support for any manager or technician facing an attack.

It provides an introduction to managing cyber attacks based on NIST and SANS models. Each step is detailed with cyber security best practices. Six typical cyber attacks are then presented to illustrate different response methods while taking into account prevention and ways of handling the attack.

Sébastien Harbec, CISSP

SMB security

Outline

Infographic: Cyber attacks on SMB

Managing cyber attacks

- Communication
- Investigation
- Containment and Eradication
- Recovery and Takeaways
- Retaining digital evidence

Different types of cyber attacks

- The phases of a cyber attack
- Network infiltration
- Data breaches
- Data encryption
- Phishing
- Compromising email inboxes
- Denial of service

List of tools

Glossary

Additional resources

References

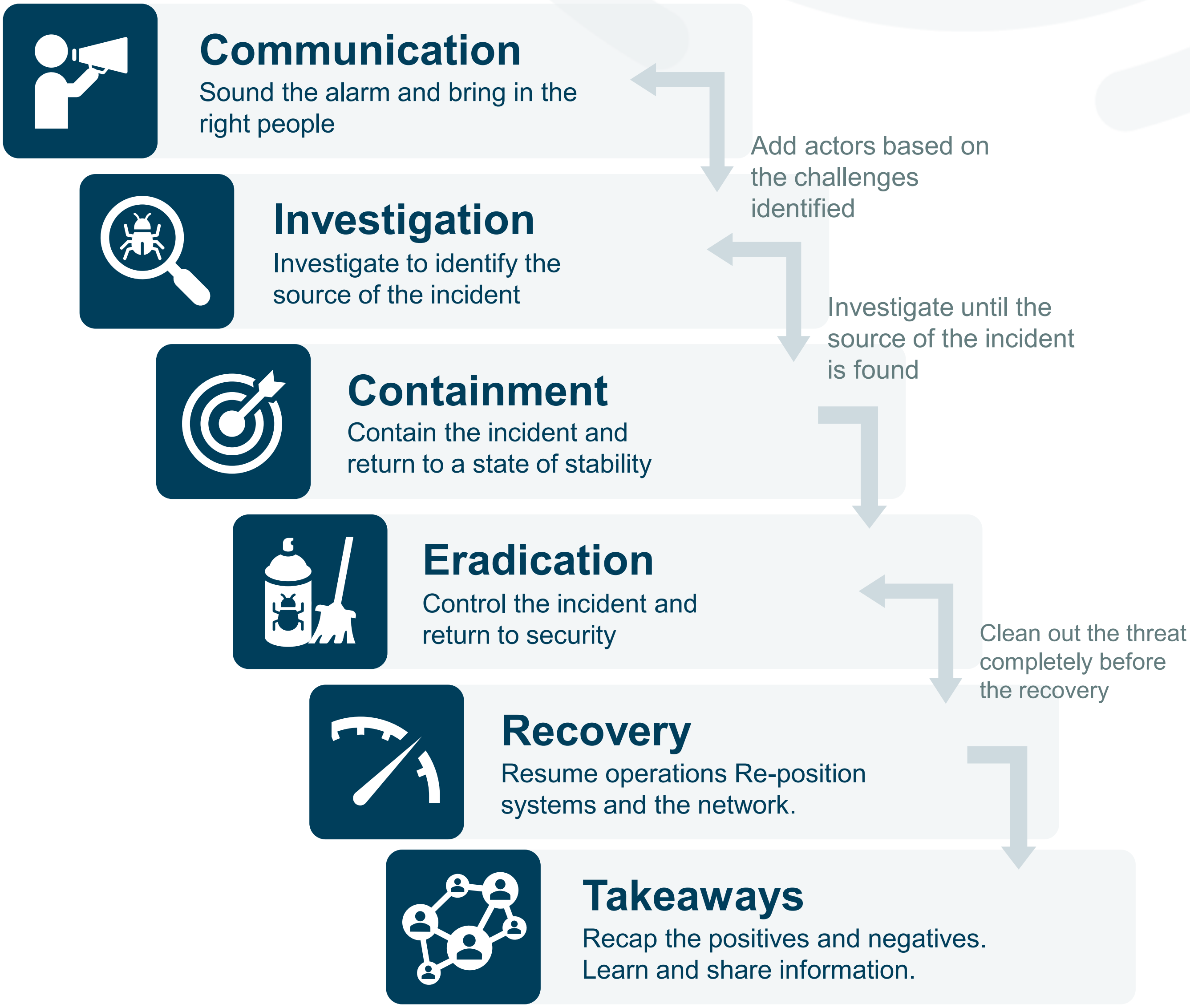
DISCLAIMER

The advice and guidance contained in this guide should not be considered to be comprehensive or all-encompassing.
It is the responsibility of systems owners to assess and assume cyber security risks that threaten their Information Technology (IT) systems.
Calling in a security expert when the situation cannot be controlled is strongly advised.

Reference: cyber.gc.ca

Managing cyber attacks

Many attacks are opportunistic and not aimed directly at a specific organisation. Instead, attackers will test all doors and open or force open those that aren't properly protected. Millions are tested daily on the Internet. "The [Canadian] Cyber Centre defines a cyber incident as any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource. Some examples of cyber incidents are phishing, ransomware and Distributed Denial of Service (DDoS) attacks." The advice provided in this document refers primarily to NIST (National Institute of Standards and Technology) and SANS (SysAdmin, Audit, Network, Security) principles for managing cyber incidents. The following reference sheets detail each of the steps shown below.



Communication

Sound the alarm and bring in the right people

Add actors based on the challenges identified

Investigation

Investigate to identify the source of the incident

Investigate until the source of the incident is found

Containment

Contain the incident and return to a state of stability

Eradication

Control the incident and return to security

Clean out the threat completely before the recovery

Recovery

Resume operations Re-position systems and the network.

Takeaways

Recap the positives and negatives. Learn and share information.

Communication

The communication aspect of an incident is very important, even critical. This includes having the right players around the table based on the level of criticality and complexity, but also communicating information properly inside the organization and possibly outside as well. Communication with clients, and possibly the media and regulatory bodies, plays an important role in the organization's reputation.

First responders

Depending on the incident detected, **the right people should be contacted quickly** based on the urgency, skills required, and possible impacts.

For example:

- A major incident could mean having to contact the business owner.
- A particularly technical incident could require contacting an expert or an external firm.
- Law enforcement, such as the police in the case of a crime, may have to be contacted.
- The person in charge of a system or business line, as well as the communications team, could also be contacted if necessary.

Sound practice

Whatever the incident, time is of the essence. That's why **it's a good idea to have a call list prepared**.

Having a list of employees and external contacts for all types of expertise, telephone numbers and availability in case of emergency will speed up the investigation and decision-making when managing an incident. This information must remain confidential.

External communication can play a strategic role for the organization, especially where its reputation is concerned. Depending on the size and type of incident, the media or clients will have to be informed. The content of the communication and how it is written will be crucial. A communication expert is therefore recommended.

You might also have to inform regulatory agencies. For example, if a data leak includes information from European clients, even if the organization is in Quebec, **General Data Protection Regulation (GDPR)** could apply, and it might be required to report to the European Data Protection Board and its Data Protection Commissioner (DPC).

Internal communication is important. Like external communication, a communication strategy will need to be put in place to determine how information will be released, to whom, and when.

There's nothing worse than uncertainty and panic when managing an incident. **Clear, transparent communication is often more effective and shows confidence in employees.** Raising awareness about the confidentiality of this information in the same communication can also be a good reminder.

Investigation

Gather as much information as possible about the incident to analyze the details and identify the source of the incident. With each finding, the right players, whether internal or external experts, must be involved in order to have the necessary expertise. It's also important to document each step and the measures taken in order to keep track of everything. To limit the damage, you can take a system offline during the containment phase and return to the investigation if necessary.

Upon discovering the incident, you have to determine the extent of the damage, like firefighters arriving at the scene of a fire.

The primary objective is to **identify the cause** of the incident in order to contain it and then fix it.

The secondary objective is to **check other network systems and devices** to see if they've been compromised.

The incident may affect the privacy, integrity and/or availability of services, systems or the network. During the investigation, you have to consider all these aspects.

- For example, crypto-ransomware attacks often involve data extraction, which affects both confidentiality and availability.

Your toolbox

Antivirus software can detect infection in a system using known and documented methodologies in the form of signatures. If a signature points to malicious behavior, the antivirus software will be able to detect the infection. This is why updates are very important, especially if you think your system has been infected.

If it has been infected, event logs can help identify the source: Internet, email, USB key or internal file.

- **Warning:** Antivirus software might not detect a sophisticated, targeted attack on a system.

Whatever the system, firewall or router, **event logs** are the place to look for anomalies. They often show details of successful and failed connections, errors and anomalies detected or changes on the system.

- They help identify abusive attempts at authentication; for example, a high volume of rejected attempts, or suspicious access to a system, outside the normal time of day, or from another country unrelated to your business.
- **But beware, they aren't always activated.** Event logs have to be activated and archived before incidents happen.

A vulnerability scan will reveal a system's weaknesses, particularly open network ports, which is the equivalent of open doors to a home.

- Some scanners can detect a large number of vulnerability details and even identify the most critical ones to repair.
- This tool can also detect an unusual change on a system, especially if you're familiar with the normal state, or basic status, of the system. Any unapproved changes from the basic status could be suspicious.
- **Careful! This tool is also used by attackers trying to identify your vulnerabilities.** If this tool is detected on your network without approval, it's very suspicious. Its use can be detected through the event logs of a system, a router or firewall alerts.

Sound practice

Test your tools before an incident to ensure that they're ready for use and that you have the right expertise. If possible, make an exact copy of the system as it was prior to the investigation and use the copy to investigate and correct the situation in order to retain the digital evidence. Don't hesitate to consult an expert if necessary.

Containment and Eradication

This phase involves **containing and eradicating** security vulnerabilities discovered during the investigation. To limit the damage, you sometimes need to quickly take a system or parts of the network offline, continue the investigation, and go back to apply patches. It's a process that can be iterative between investigating new flaws and applying patches until the incident is resolved. When applying patches, many organizations use this opportunity to improve their overall security.

Containment can be used to contain the incident quickly based on the knowledge gained during the investigation to take action and prevent the incident from spreading.

Before taking action on a system, if **digital evidence** must be retained, it's best to make an exact copy of the system and use that copy to make any changes.

It may be necessary to immediately **isolate a system**, for example, when a system is compromised with a virus, and suspicious communication is detected through the firewall. It's also a way to prevent systems that are still healthy from becoming affected.

- This is an emergency procedure and should only be used with awareness of the impact on the services offered, e.g. a web server.
- Isolation can be done via a network configuration from the firewall or router, or by unplugging the network cable.
- Isolation can make the investigation more difficult since it will put an end to the suspicious communications from outside the organization. If possible, the analysis should therefore be done prior to isolation.
- In addition, this alters the condition of the computer and must be duly noted if digital evidence must be retained.

Once isolated, the system should be stabilized unless an infection is already in progress.

Antivirus software lets you make an initial diagnosis and sometimes disinfect the system.

Special cases occasionally require more advanced antivirus software called anti-malware. This tool is often an excellent supplement during the disinfection stage. *See the Tools sheet.*

A vulnerability scan will identify a system's weaknesses and often recommend a solution. It's a great tool to determine priorities for patches.

- Patches can be system, network or application configurations.

Application and system updates can be among the patches to be applied. Keeping your systems and applications up to date is a great way to protect yourself.

By the eradication stage, the incident should be under control.

This step comes just before systems return to normal, so make sure that all systems are intact and free of infection. This isn't a temporary patch, but a permanent fix.

- The same tools as during the containment stage can be used, but a higher level of assurance will be expected to make sure no significant or critical vulnerability remains on the system to prevent it from being attacked again.
- A new configuration, new system or major architectural change could be required to achieve a satisfactory level of security depending on the size of the service that's been affected.
- Eradication can be a technical step and can require special expertise, so be sure to consult an expert when necessary.

Pay attention to change management Any changes, systems updates and applications can result in system instability and cause an incident. It's important to carry out the necessary stability tests before restarting services.

Recovery and Takeaways

Once the fixes have been applied, operations can resume. Several best practices can be adopted at this point. Moreover, surveillance and security testing must continue to make sure the attack is over.

Operations can resume quickly if there's a backup copy for the infected system(s).

- If a recent backup is available, make sure it doesn't present a security issue before redeploying it.
- If possible and if necessary, deploy the backup image to a second system to maintain digital evidence on the original system. This will also help to investigate the system and install its replacement.
- For desktops, a standard image of the system is often kept. If the data is centralized on a cloud or internal server and the data has not been affected by the attack, workstation recovery will be relatively quick.
- For network equipment such as a firewall or router, recovery from a backup is also possible if the backup is recent. You still have to make sure this backup is intact and functional and that it hasn't been maliciously manipulated.
- If there's been any malicious manipulation, you have to think about service interruption, backup integrity, and whether the backup data is fairly recent.

Be careful! Several backup solutions are effective for making backups, but very complex for restoring data. Backup restoration should be tested regularly.

Once operations resume, it's a good idea to perform a weekly vulnerability scan on all the systems in the environment.

- This will give you an overview of the systems' security and vulnerabilities in order to prevent, or discover, new attacks.

Application and system updates must be part of day-to-day operations to ensure operations are resumed efficiently. Without these updates, it's very difficult to guarantee system security.

The takeaways stage is essential to ensure that the return to normalcy is complete, effective and long-term. The goal is to learn from mistakes made and successes achieved during the incident.

- Include everyone involved in resolving the incident.
- Gather all the documentation produced during the incident.
- Indicate the improvements, challenges, mistakes and successes.
- Sharing this information with your industry peers is also a beneficial way to improve and build trust.

Sound practice

Similarly, tabletop exercises are recommended to simulate incidents and discuss or test responses. If a process isn't working as intended or something is missing, it will become apparent at this point.

Retaining digital evidence

Digital evidence must be retained primarily within a legal framework in the event the organization wants to seek legal recourse for an incident. Ideally, the principle of retaining evidence should be followed for all suspicious incidents since it could be discovered during the course of the investigation that the incident was an attempt to defraud, steal from or harm your organization. The best practices set out in this document are high level. You should therefore call on a legal expert to make sure that the principles and laws are properly applied. In some cases, law enforcement may also have to be called in.

Retaining evidence starts with the importance of documenting. It must be organized from the outset of the incident and include all relevant information. You would be advised to use an incident documentation tool, form or framework to make sure you have all necessary information. (See the Tools sheet) All material evidence must also be clearly labeled and stored with limited and documented access to maintain its integrity.

All evidence must be traceable, especially when it's shared. Each transfer must be documented and include the signature of all parties, the date, time, subject matter and technical details for equipment or system access, where the information will be hosted, and the number of access rights.

No modifications should be made so that system integrity is maintained throughout the investigation. Some computer analysis and investigation tools can be used to analyze the system without modifying it and make an exact copy of the hard drive. (See the Tools sheet.)

- An exact copy of the hard drive can be used in the investigation or to perform correction and recovery tests while preserving the state of the original system.
- If the system need to be isolated from network and Internet it is preferable to use the firewall or router to limit changes to the system itself. Document and think carefully before undertaking such a change, since this will still change the system's communications states.
- If the system must be switched off, don't use the system or shut down the computer normally. Instead, turn off the power supply in order to maintain the state as is. This should be avoided as much as possible since it can also physically damage the system.

Analysis in random access memory or RAM can be very useful in an investigation. It's volatile, meaning that it's erased when the computer restarts or sometimes when it goes to sleep. Like the hard drive, the memory can be analyzed directly on the system without disrupting its state. However, a copy should be made and analyzed on a second system with memory analysis tools. (See the Tools sheet.) Some attacks can be found only in RAM through the system's processes or executed files.

It also lets you see:

- Some network communications
- What's been copied/pasted, including some passwords, if applicable
- Whether any malicious command lines have been recently executed.
- In more complex cases, it can show whether code has been injected into the system to exploit it.

Retaining digital evidence must be simple and effective. If the process of accessing evidences via a computer system can be automated, it will be easier to follow and review later. If the process is done manually, it could be neglected, forgotten or worse, overridden.

- Many investigations become very complex when the volume of information is overwhelming. It may be a good idea to put at least one person in charge of ensuring that the principles for retaining digital evidence are followed throughout the process. Anyone who handles or has access to information related to the investigation should be familiar with the evidence retention process to ensure its integrity.

Cyber attacks

Now that we've seen the steps involved in managing a cyber attack, let's look at some typical attacks. In security, the level of risk for each step is calculated in relation to your likelihood of being attacked, the impact on your business, and your organization's security controls. Keep in mind that vulnerability exploitation is often blind and that the majority of attacks are opportunistic. If your defenses are weak, an attack is much more likely. Attackers and fraudsters therefore tend to choose targets that are fairly easy and obvious.

Network infiltration

Intrusion into your network is often the beginning of an attack through various means.

Data breaches

Your sensitive data is extracted:
client base, sales or intellectual property.

Crypto-ransomware

Your data and systems are no longer accessible.
You receive a demand for ransom!

Phishing

You receive sophisticated fraud emails asking for your banking or personal information.

Compromising email inboxes

Fraudsters have access to your email inbox
in order to embezzle funds or steal information.

Denial of service

Your systems slow down or shut down completely affecting your operations and your services.

Objectives

How to detect this type of fraud

What to do

Sound practices

The phases of a cyber attack

There are several types of cyber attacks, and they each use different strategies to obtain financial gain or to attempt to do harm. According to Lockheed Martin, **there are 7 steps in a cyber attack**. Depending on the attack, some will be faster or slower than others. These phases provide a better understanding of how an attack is carried out and help in managing the incident.

1 Reconnaissance

The attacker looks for information about the organization. This information is mainly in the public domain, or is easily accessible. This phase should help identify how the attack will be carried out. Here are some examples:

- Employees' email addresses
- Looking up information about the company
- Looking up information about individuals
- Identifying external vulnerabilities
- Visiting the company on a reconnaissance mission, pretending to be a delivery driver, for example.

2 Weaponization

The attacker creates or chooses a tool to exploit a detected vulnerability or flaw. The tool can exploiting a flaw to target a system as easily as a human being by using social engineering techniques.

3 Delivery

An infected email attachment, virus or worm is sent to the organization's network.

4 Exploitation

A vulnerability or weakness is exploited to obtain an initial gain. This step could lead to further access rights to a system. In phishing, an attacker captures a system administrator's credentials, for example.

5 Installation

A backdoor is installed. Even if the vulnerability is fixed, a backdoor installed on a system and accessible from the Internet will allow the attacker to gain persistent access and initiate the next steps.

6 Command and control

From the backdoor, the attacker will have permanent access and can take and give orders remotely depending on the access rights acquired on the system.

7 Actions on objectives

In the last step, attackers use the backdoor and execute commands to accomplish their objective. This can involve:

- Stealing data for espionage, resale or in exchange for a ransom
- Encrypting data, called crypto-ransom
- Modifying information for their benefit
- Stealing or embezzling money, for example, via bank transfer

We'll also cover APT, which stands for Advanced Persistent Threat. This refers to an attacker who goes through all the steps identified here and stays on your organization's network and systems. This way, the attacker can act more slowly to avoid being detected or to execute a much more complex scheme. Some persistent attacks can take organizations years to detect and defeat. In these situations, the impact on the company is often significant.

Network infiltration

Network infiltration has a fairly broad meaning. It basically means that an attacker has broken into the computer network, or actively tried to, by exploiting a weakness from the Internet, your website, an application, or even by impersonating an employee for example. Once in the network, the attacker will try to move around, exploiting all kinds of vulnerabilities to reach their target.

How to detect this type of fraud

Network infiltration is often one of the steps involved in a cyber attack. It's generally difficult to detect unless surveillance systems are already in place. It can be found out, for example if suspicious connections are discovered on the network.

Here are a few things to watch for

- **Unusual connections** on the router or firewall, such as connections from a country you don't do business with.
- **Uncommon actions**, such as a large data transfer or activity outside of business hours.
- **Recently created user accounts.**
- **Files or software** added or deleted on a system for no reason.

⚠ **Be careful!** Hackers can also cover their tracks to make discovering them more difficult. If you suspect intrusion in a specific system, then you also have to investigate the system through the event logs. If they haven't been modified by the attacker, they can confirm the intrusion.

Sound practice

Automatically transfer all event logs to a centralized server. This makes it easier to investigate an incident because you can conduct your investigation without logging into the potentially compromised server.

What to do

Once the attack and the source of the breach have been identified and investigated, depending on its magnitude, your company may initiate the appropriate incident management process.

Here are a few steps that can help you deal with this type of attack.

❶ Contain

- Disconnect potentially compromised systems from the network and the Internet.
- Cut off and block suspicious network connections.

If the previous investigation is complete, the hacker no longer has access to the network or systems.

❷ Retain

- Make an exact copy of potentially affected systems. It can be used in a forensic investigation, if necessary.

❸ Recover and eradicate

- If there's a backup copy of the affected systems, it can be used to restart a copy of the system.
- Before reconnecting the system to the network, make sure it has been completely cleaned.
- **Using antivirus software and a vulnerability scanner is recommended.** Further investigation may be necessary.
- Only once the system integrity has been validated, it can be reconnected to the network and the Internet if applicable.

Data breaches

The objective of a computer attack can be to steal data. In most cases, it's for financial gain. The data is often used for identity theft. It could also be intellectual property theft to steal your corporate secrets. The thief could then resell this information, including your client list and sales figures, to the highest bidder on the Internet. Data leaks can also originate from within, i.e. initiated by an employee, consultant or third party. A leak can be the result of a handling error, an employee working from home, information shared externally, or malicious intent.

How to detect this type of fraud

Data theft can be detected when data is extracted from or leaves your network. Data leak detection systems, often called DLP for Data Leak Protection, help detect and sometimes even block leaks. If you don't have a DLP system, watch for these clues.

- **Monitor Internet consumption** for abnormal volume. Information is available on your Internet provider's website or your network firewall or router.
- **Monitor outbound Internet activities and connections outside of office hours**. Information normally available on your corporate firewall or router.
- **Check whether your email system already has data leak detection or prevention rules** for email attachments. This can create alerts easily.

Leaks can happen in a number of ways:

Through the use of USB keys, CD/DVD burning, email attachments (professional or personal), storage sites, such as OneDrive, Dropbox and GoogleDrive, for example.

⚠ **Be careful!** If criminals want to cover their tracks, they might use file encryption. It takes a password or the original file on the system used to discover content.

What to do

Take control of the information

- If the information has ended up on the Internet, you have to take control of it quickly and try to delete it.
- If it was the result of an employee's error, it's often quicker to ask the employee to delete it directly than to contact the website managers, although this will be necessary in some cases.
- You can look up the email address and phone number to call by doing a WHOIS search. You can do this type of search on several websites. In Canada, you can use CIRA at cira.ca.

Sound practices

- **For remote work, secure access by VPN (secure tunnel) should be used** instead of email attachments. Once a confidential file is sent by email, it's hard to keep track of it.
- **Make sure employees understand what is confidential** and the importance of not letting information out of the company.
- **Close data output accesses where possible:** USB ports, CD/DVD burners, email and storage sites could also be blocked if they're not needed for employees to do their work.

Crypto-ransomware

A computer attack could involve encrypting the company's data. The hacker's goal is to encrypt the data to make it inaccessible to the company. They then send a ransom request demanding payment in exchange for the password or decryption key. But beware: data decryption isn't always successful, it can take a lot of time, and the ransom can be very high. In some cases, ransoms for larger companies run in the millions. Not to mention that paying ransom is like financing the cybercrime industry, which enables them to carry out even more sophisticated computer attacks!

How to detect this type of fraud

Detecting an encryption attack is usually quick and easy. The affected systems no longer respond, and very often a screen will display the ransom demand and payment process. No action will be possible.

⚠ **Beware** of fake ransom demands! Some malware displays a screen like this one but doesn't actually encrypt computer data. Simply restart the computer with standalone antivirus software on a USB key or CD. See the Tools sheet.

Sound practice

Encryption malware often arrives via email through an attachment or link to a malicious site. The infection can also happen through an infected website or with a USB key.

The best approach to protect yourself is to back up data off-network, and even off-site. In the case of a major infection, the backup will be protected.

What to do

❶ **Disconnect the infected system from the network and the Internet** to prevent reinfection and keep the virus from spreading.

❷ **Making a copy of the infected system** is always a good practice if an in-depth investigation is necessary.

❸ **Determine the cause of the infection** especially if it comes from another system or poorly protected Internet access.

❹ **Try to restore your information**

- Make sure the backup hasn't been infected. Ideally, test it on another "empty" system.
- Then use antivirus software to validate and install the backup on the affected system.
- If all goes well, the new system will be free of encryption.
- Before reconnecting it to the network and the Internet, you should apply all system updates and install antivirus software.

❺ **What if you don't have a backup or it's infected?**

- Try to disinfect the system. Use a reboot disk for antivirus software. See the Tools sheet.
- This allows the machine to restart under the control of the antivirus software, do a diagnosis and attempt disinfection.
- For some well-known encryption software, there are disinfection solutions. Simply identify the software and search for the solution on the Internet.

Phishing

The term phishing comes from the analogy of attackers fishing for information by selecting one or more victims. Phishing can be carried out by phone or through impersonation (e.g. FedEx delivery driver) but very often takes place via email. The objective of the attack is to obtain sensitive information, such as username and password, answers to secret questions, or confidential information about the victim or their employer.

How to detect this type of fraud

It isn't not always easy to distinguish between a phishing email and an authentic email. Years ago, malicious emails were full of spelling mistakes, often in English, and contained many clues that flagged them as "phishy." Now, fraudsters address you in your language, without errors, and make reference to matters that concern you.

When trying to identify a malicious email, look for the following warning signs:

Do you know the sender, and were you expecting an email from them?

- An email, even from a friend or colleague, can be a phishing attempt. They may have been hacked, and now the hacker is trying to reel you in.

Does the email use an unusually URGENT, insistent tone?

- This is a fairly common sign of phishing emails.

Are you being prompted to change your password, pay a bill, open an attachment, or click on a link?

- **Be careful!** This is very suspicious! If there's a link, hover your mouse over it without clicking to see the website it's actually redirecting you to.
- **Be careful!** These sites are often ones you've never heard of, but sometimes they're sites you recognize but with a typo! (e.g. Gooogle.com or Yahao.ca).

What to do

❶ If you receive a phishing email, the best thing to do is **delete it or report it to your IT team** or through your email software. Often it's as easy as right-clicking and selecting "Report Phishing."

❷ If the email link or attachment has been opened, **disconnect the computer from the Internet and network** and treat it as infected until you have proof that it isn't. Then **scan it with antivirus software** to ensure the computer's integrity. **See the Tools sheet** for advice.

❸ If the email redirects a user to a page where they're asked to enter a username and password and they do, they should change them immediately. Another good practice is to disable the user account on the network, if necessary. You'll also have to investigate to make sure the authenticators haven't already been used with malicious intent. A technical analysis may be required.

Sound practices

- Providing employees with **training** on phishing makes a difference when it comes to recognizing a fraud attempt and avoiding clicking. Running fake phishing email campaigns for employees while adhering to privacy ethics is also effective.
- The best strategy with phishing is to **be careful, ask yourself the right questions before clicking**, and if in doubt, don't open them.

Compromising email inboxes

Compromising email inboxes is an increasingly common attack in all types of business. This enables fraudsters to access and take control of an email inbox and often includes receiving, intercepting and sending spam emails. It also gives them access to information that's already in the inbox, not to mention all possible access rights by changing the password from the email inbox. The objective can also be monetary: changing banking information when a transfer is carried out.

How to detect this type of fraud

This type of attack can be rather difficult to detect. Often, when the incident is detected, it's already too late: the fraudster has already taken control of the emails and is acting for their own gain.

Typically, **this type of attack occurs as a result of phishing**, so that the fraudster can obtain the password of the person being targeted. In other cases, it can occur when an old password is leaked and reused on another website.

Here are some clues that an email inbox has been compromised:

- The email inbox has been accessed outside of business hours, from other countries.
- Emails to foreign recipients are unusual.
- New email inbox rules automatically redirect emails to an external address (the fraudster's), another folder, or trash can.
- Fraudulent emails are received from this email inbox.

What to do

As soon as you realize the email inbox has been compromised, you should:

❶ **Immediately change the password or disable the email inbox temporarily** so that the investigation can take place.

❷ **Understand what was done by the person whose email inbox was compromised** in order to detect the source of the problem and correct it. It may be necessary to quarantine the computer to make sure there's no further infection.

❸ **Investigate what the fraudster did**, e.g. added new redirect rules sent fraudulent emails.

❹ **Check whether any other email inboxes have been compromised.**

Sound practices

Using two-factor authentication, such as software token, when connecting to an email inbox from outside the office greatly reduces the risk of compromise. This is often available from your email hosting provider.

Using complex passwords is also important for preventing this type of fraud.

Having a unique password for each service is also essential. An old password that's been leaked could be used against you.

Denial of service

The objective of this attack is to render a company's resources or services unavailable. The target can be the company's website, email service, printing, and often Internet access. Typically, the attacker will try to overload a system, for example, by flooding it with multiple requests or making malformed requests to shut it down so that it can't respond to normal requests. This type of attack can also be accompanied by a ransom demand.

How to detect this type of fraud

- **When a service has been stopped, it doesn't automatically mean it's a denial-of-service attack**. However, the first signs could be similar.
- The cause of the problem must be **investigated** to see if it's a slowdown caused by a glitch, a technical error such as a bad configuration, or simply higher-than-usual volume.
- **The services targeted are often those that affect the company the most**, such as its website, especially if it's a transactional site.
- **A ransom demand may arrive** by email before or after the attack.

⚠ **Be careful!** Fake ransom demands can threaten with a denial of service attack if the payment demanded isn't made, in which case you have to determine whether the threat is real.

Sound practices

Website hosts and Internet service providers sometimes have protection against this type of attack.

For in-house web hosting, there are several solutions: **load balancing**, which distributes requests, **firewalls** that can block illegitimate requests, or **cloud solutions** that redirect and analyze traffic to detect and prevent this type of attack.

What to do

System slowdowns or shutdowns must be investigated systematically. You have to investigate the most probable cause based on the signs, very often embedded in technical details. To perform the diagnosis, you need to ask a number of questions.

For example:

- **Has the affected device or service undergone a recent technical change?**
- **Could the system be legitimately overloaded (e.g. special sale)?**

If a denial of service is suspected, an investigation will have to be done quickly on the firewall or router. **If an abnormal number of requests arrive from a single destination, the culprit will be easy to identify** and can be blocked quickly.

However, **expert hackers will instead spread their attack and use multiple sources**. It's harder to block this type of attack without affecting the availability of your own service.

Using a protection service against this type of attack is often the best solution. Technical expertise may therefore be necessary.

Tools

Here are the various tools you need to monitor, investigate, correct and contain a number of security issues. It is recommended that you understand these tools and have the expertise to use them in order for them to be effective when an incident or investigation needs to be handled quickly.

Type	Advantages	Advice	Characteristics
Antivirus software	• Necessary protection for known viruses and attacks. • Works very well when the signature of the attack is known.	• Updates are essential in order to have a database of the latest signatures.	• The antivirus will quarantine and block certain threats that can be recognized by a signature.
Reboot disk for antivirus analysis	• Perfect for isolating and investigating a system quickly and attempting to disinfect it.	• Disconnect the system from the network as soon as possible to prevent the infection from spreading.	• Allows you to start up an infected computer on a standalone operating system based on antivirus software.
Anti-malware **Anti-ransomware**	• This type of software complements antivirus software and focuses on malware threats.	• If integrated into antivirus software, it must be proven effective against malware and ransomware threats	• This is a great complement to antivirus software and detects and cleans other types of malware
EDR Endpoint Detection and Response	• Complements antivirus software. Speeds up the investigation and threat remediation.	• Integrate it into logging and log event detection tools. • Should be able to detect anomalies in system behaviour.	• EDR is better at monitoring abnormal and malicious behaviour than traditional antivirus software. It's a very good complementary tool for emerging threats.
Digital investigation software	• Makes incident management easier when digital evidence needs to be preserved.	• Understand and test the tool.	• Documentation and investigation tool which, if used properly, complies with the rules of retaining evidence.
Memory forensics **(Expert required)**	• Makes it easier and faster to do an in-depth investigation of a system.	• Requires a level of technical expertise.	• With this tool, you can see information in the random access memory, such as most recent commands used, password, etc.
Vulnerability scanner **(Technical level)**	• Identifies vulnerabilities on systems and applications. Often suggests corrective solutions.	• Watch out for false positives. The volume of vulnerabilities can be high. Distinguishing between real and fake requires technical expertise.	• An online scanner (Internet) identifies vulnerabilities on the infrastructure from an external standpoint (web and perimeter). • An in-house scanner will validate a more detailed and accurate level of vulnerabilities.
SIEM Security information and event management	• Speeds up investigations and the correlation of security events	• In order for SIEM to be effective, the right log events must be included. • Use cases or alert scenarios must be in place.	• Allows all security events to be centralized in one place.

Glossary

Availability

The ability for the right people to access the right information or systems when needed.

Confidentiality

The ability to protect sensitive information from being accessed by unauthorized people.

Encryption

Converting information from one form to another to hide its content and prevent unauthorized access.

Firewall

A security barrier placed between two networks that controls the amount and kinds of traffic that may pass between the two.

Flaw or vulnerability

A security flaw is a weakness that emerges because of negligence or a deliberate attack. It can run counter to a policy or law and is often exploited to perpetrate harmful or criminal actions.

Integrity

The ability to protect information from being modified or deleted unintentionally.

Malware

Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.

Ransomware

A type of malware that denies a user's access to a system or data until a sum of money is paid.

Router

A networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. There are some simple rules that block or filter connections between the networks or with the Internet.

https://cyber.gc.ca/en/glossary

Additional resources

Cybereco

Cybersecurity awareness kit

https://cybereco.ca/en/business-kit/

Business Development Bank of Canada

Your checklist for avoiding IT security breaches

https://www.bdc.ca/en/articles-tools/technology/invest-technology/computer-security-checklist-small-businesses

Canadian Centre for Cyber Security

Get Cyber Safe

https://www.getcybersafe.gc.ca/en/resources

Canadian Centre for Cyber Security

Baseline Cyber Security Controls for Small and Medium Organizations

https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Canadian Centre for Cyber Security

Develop an Incident Response Plan

https://cyber.gc.ca/en/develop-incident-response-plan

References

MicroAge, The True Costs of a Cyberattack and how to Best Respond
https://www.microage.ca/wp-content/uploads/2019/09/The-True-Costs-of-a-Cyberattack-and-How-to-Best-Respond_eBook.pdf
VERIZON, 2020 Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/dbir/
GOVERNMENT OF CANADA, CANADIAN CENTRE FOR CYBER SECURITY, Get Cybersafe
https://www.getcybersafe.gc.ca/en/resources
GOVERNMENT OF CANADA, CANADIAN CENTRE FOR CYBER SECURITY, Baseline Cyber Security Controls for Small and Medium Organizations
https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations
WIKIPEDIA, Router
https://en.wikipedia.org/wiki/Router_(computing)
HISCOX ,Hiscox Cyber Readiness Report 2019
https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF
RADIO-CANADA, Les PME québécoises trop vulnérables aux cyberattaques
https://ici.radio-canada.ca/nouvelle/1164074/cyberattaque-cybersecurite-piratage-informatique-pme-entreprises-quebec
STATISTICS CANADA, Cyber security and cybercrime challenges of Canadian businesses, 2017
https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-eng.htm
L'INFORMATION D'AFFAIRES D'ICI, Cybersécurité: les PME exposées aux mêmes menaces que les grandes entreprises
https://infodaffaires.com/cybersecurite-les-pme-exposees-aux-memes-menaces-que-les-grandes-entreprises/
LA PRESSE, Attaques contre les PME: un nouveau chien de garde en sécurité informatique
https://www.lapresse.ca/affaires/entreprises/201911/29/01-5251721-attaques-contre-les-pme-un-nouveau-chien-de-garde-en-securite-informatique.php
RADIO-CANADA, Les PME québécoises trop vulnérables aux cyberattaques
https://ici.radio-canada.ca/nouvelle/1164074/cyberattaque-cybersecurite-piratage-informatique-pme-entreprises-quebec
CYBERSEC&YOU, Cybersécurité des PME : comment les accompagner vers la prise de conscience ?
https://www.cybersecandyou.com/cybersecurite-des-pme/
UNIVERSITÉ DU QUÉBEC, L'IMPORTANCE DE LA CYBERSÉCURITÉ POUR LES PME
https://www.uquebec.ca/reseau/fr/medias/actualites-du-reseau/limportance-de-la-cybersecurite-pour-les-pme
GLOBAL SECURITY MAG, Cyber readiness levels stall as attacks reach new intensity International study shows no improvement in corporate defences despite soaring cyber losses,
https://www.globalsecuritymag.fr/Cyber-readiness-levels-stall-as,20190423,86426.html
CCI ALPES DE-HAUTE-PROVENCE, Comment réagir en cas d'attaque informatique ?
http://www.digne.cci.fr/IMG/pdf/Fiche_23_-_Securite-Comment_reagir_en_cas_d_attaque_informatique.pdf
CSO ONLINE,How to report a data breach under GDPR
https://www.csoonline.com/article/3383244/how-to-report-a-data-breach-under-gdpr.html
SANS, Memory Forensics Analysis Poster
https://digital-forensics.sans.org/media/Poster_Memory_Forensics.pdf
BDC, Your checklist for avoiding IT security breaches
https://www.bdc.ca/en/articles-tools/technology/invest-technology/computer-security-checklist-small-businesses
GOVERNMENT OF CANADA, CANADIAN CENTRE FOR CYBER SECURITY, Develop an Incident Response Plan
https://cyber.gc.ca/en/develop-incident-response-plan
NIST, Computer Security Incident Handling Guide
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
NIST, Guide to Integrating Forensic Techniques into Incident Response
https://csrc.nist.gov/publications/detail/sp/800-86/final
AT&T, Incident Response Steps and Frameworks for SANS and NIST
https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide
USA, FEDERAL TRADE COMMISSION, Data Breach Response: A Guide for Business
https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business
COMODO, Does Paying Ransomware Work?
https://enterprise.comodo.com/does-paying-ransomware-work.php
FBI, SCAS AND SAFETY: Ransomware
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
LOCKHEED MARTIN, Proactively Detect Persistent Threats
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

cyber eco